УДК 330.101 DOI: 10.14451/1.259.19

Киберриски как системная угроза экономическому суверенитету

© 2026 **Людвиг Лидия Петровна**
Кандидат экономических наук, доцент, кафедра Экономическая безопасность и таможенное дело. Сахалинский институт железнодорожного транспорта — филиал Дальневосточного государственного университета путей сообщения, Россия, Южно-Сахалинск.
E-mail: llpjob@mail.ru

© 2026 **Медведева Дарья Евгеньевна**
Студент. Сахалинский институт железнодорожного транспорта — филиал Дальневосточного государственного университета путей сообщения, Россия, Южно-Сахалинск.
E-mail: HelloDude490@mail.ru

Ключевые слова: цифровизация, киберриски, экономические последствия, информационная безопасность, дезинформация, цифровая экономика, экономическая безопасность, киберустойчивость.

В статье исследуется трансформация киберрисков из операционной проблемы в стратегическую угрозу экономической безопасности государства. На основе анализа статистических данных выявлены устойчивые тенденции в эволюции киберугроз и их каскадное воздействие на различные отрасли экономики. Предложен комплекс практических мер, направленных на формирование системы киберустойчивости, и доказана их экономическая целесообразность в контексте предотвращения системных кризисов.

Введение

«Связующим звеном в современной цифровой экономике при формировании инфраструктурных процессов являются интернет, облачные IT-технологии, реализуемые посредством специализированного программного обеспечения» [4, с. 269] — это актуализирует вопрос относительно обеспечения кибербезопасности для экономического суверенитета государства, фундамент которого составляют компании реального и финансового секторов. Дестабилизация их работы в результате киберинцидентов: будь то масштабная утечка конфиденциальных данных или продолжительные операционные простои — способна спровоцировать не просто локальные убытки, но и системный кризис.

Подобные инциденты порождают каскадные эффекты, нарушая стабильность цепочек поставок, подрывая доверие инвесторов, оказывая сильное влияние на капитал компании и дестабилизируя национальную финансовую систему в целом, что находит свое подтверждение в ряде ситуаций, которые подробно раскрыл Forbes в своей статье «Шантаж и шпионаж: какие киберриски угрожают бизнесу и пользователям в 2025 году»: «...в 2024 году обнаружены продажа девяти корпоративных доступов стран СНГ и сообщение с бесплатной «раздачей» 21 доступа

к российским компаниям...» [8]. Помимо прочего, в данной статье также подтверждается факт влияния киберрисков не только на крупные, но и на более мелкие компании или поставщиков и подрядчиков, которые имеют менее развитую систему информационной защиты, что кратно повышает актуальность нашего исследования.

Также особенное влияние оказывает растущая сложность негативного воздействия киберугроз, изощренность которых напрямую коррелирует с развитием IT-технологий, мощным драйвером которых в последние годы стали алгоритмы искусственного интеллекта и нейросетевые модели, используемые, в том числе, и самими злоумышленниками. Это создает для нас особый вызов, заключающий в разработке эффективных механизмов защиты.

Целью настоящего исследования является комплексный анализ природы киберрисков и оценка масштабов их деструктивного воздействия на все уровни экономики: от микроуровня отдельных предприятий до макроуровня государства.

Гипотеза исследования заключается в следующем: в условиях цифровой трансформации киберугрозы эволюционировали в качественно новую угрозу - они характеризуются не точечным, а комплексным и каскадным влиянием, способным не только подорвать финансовое состояние конкретных корпораций, но и деформировать конкурентную среду, а в перспективе - поставить под вопрос экономическую независимость и безопасность страны.

Для достижения поставленной нами цели и подтверждения или опровержения гипотезы, выдвинутой ранее, нам необходимо решить ряд задач.

Во-первых, систематизировать и охарактеризовать современную типологию киберрисков, выявив их специфические черты в отличие от традиционных экономических угроз.

Во-вторых, проанализировать механизм и оценить степень влияния киберрисков на микро- (отдельные компании) и макроуровнях (отрасли, регионы, национальная экономика).

В-третьих, выявить и смоделировать каналы трансмиссии киберугроз между различными секторами экономики, оценив потенциал возникновения негативных синергетических эффектов.

В-четвертых, разработать комплекс практических рекомендаций для органов государственной власти и частного сектора, направленных на минимизацию вероятности реализации киберугроз и смягчение их экономических последствий.

Материалы и методы

Эмпирическую базу нашего исследования составили научные публикации за последние пять лет и статистические данные платформы Solar — сочетание теоретического и статистического анализа позволит не только диагностировать текущее состояние проблемы, но и разработать практические рекомендации по ее дальнейшему снижению.

В качестве методов исследования применяются анализ, синтез, классификация киберрисков и сопоставление статистических данных. Комплексное использование представленных методов направлено на разработку эффективных способов управления экономическими последствиями киберрисков.

Результаты

Экономический суверенитет представляет собой способность компании или государства в полной мере контролировать свои ресурсы, экономическую политику и финансовую систему, он также находит свое отражение в независимости от воздействия извне.

Важно отметить, что экономическая независимость первоочередно формируется из устойчивости ключевых национальных или корпоративных активов к внешним и внутренним шокам — эта устойчивость, в свою очередь, складывается из нескольких фундаментальных компонентов, включающих в себя:

1. Технологический суверенитет, то есть обладание независимыми и конкурентоспособными технологическими решениями в критически важных отраслях, от микроэлектроники

и софта до телекоммуникационной инфраструктуры;
2. Кадровый потенциал, обеспечивающий не только разработку и внедрение этих технологий, но и формирование культуры кибербезопасности на всех уровнях;
3. Эффективная система управления рисками, включающая в себя стратегическое прогнозирование, механизмы быстрого реагирования на инциденты и финансовые «подушки безопасности» для минимизации ущерба.

Именно в этом контексте киберриски предстают как прямая угроза экономическому суверенитету, поскольку саботаж цифровой инфраструктуры или утечка стратегических данных подрывают все перечисленные выше компоненты, переводя контроль над активами и процессами к внешним злоумышленникам или конкурентам, тем самым ставя под сомнение возможность независимого экономического развития и повышая издержки.

Таким образом, «Киберриск — риск, обусловленный невыполнением требований по обеспечению безопасности цифровой информации» [10, с. 30]. Сущность киберриска и формирует его отличие от других видов рисков: финансовых, производственных, традиционных (привязанных к определенной юрисдикции или физической инфраструктуре).

Следовательно, ключевые особенности киберрисков включают транснациональный характер атак с асимметрией ущерба, динамичную эволюцию угроз, требующую постоянного адаптивного управления, и материализацию последствий в физическом мире.

Отличительными чертами являются также латентность инцидентов, сложность атрибуции и значительный потенциал внутренних угроз.

Таким образом, киберриски формируют системную угрозу с комплексным воздействием на экономику и требуют принципиально новых подходов к управлению безопасностью, а наш тезис находит свое отражение в отчете Solar: «Инциденты с высокой степенью критичности могут привести к значительному как финансовому, так и репутационному ущербу для бизнеса (например, длительные простои, прерывание ключевых бизнес-процессов и деятельности в целом)» [6].

Наибольшую опасность представляет латентный характер киберинцидентов, приводящий к запоздалому обнаружению атак и значительному росту ущерба, к ключевым угрозам относятся: компрометация данных, нарушение целостности информации и репутационный ущерб.

В современных условиях репутация становится критически важным активом, поскольку потребители проявляют повышенную чувствительность к имиджу компаний, распространение порочащей информации в свою очередь подрывает доверие к организации и напрямую влияет на её финансовые показатели.

Таким образом, среди наиболее частых киберугроз находят своё отражение [5]:

1. DDoS-атаки — попытка вывода из строя сайта или онлайн-сервиса путем массовой отправки запросов с множества устройств;
2. Шифровальщики — вредоносное ПО (ВПО), блокирующее или шифрующее доступ к вычислительным ресурсам пользования, вследствие требующее выкуп за восстановление доступа или дешифровку;
3. Стиллеры — ВПО, похищающее данные для последующей отправки злоумышленнику;
4. Сайты-ловушки (распространение ВПО через веб-ресурсы в том числе) — мошеннические ресурсы, направленные на кражу денег или персональных данных пользователя;
5. Тайпсквоттинг — метод кибермошенничества, заключающийся в создании сайта на домене, схожем с названием оригинала для обмана сторонних пользователей;
6. LNK-файлы — используются в киберпреступности для доставки ВПО, попадают через подозрительные загрузки или вложения в электронных письмах, при открытии которых система Windows незаметно исполняет нежелательные команды, несущие в себе вредоносный код;

7. ClickFix — использование поддельных систем проверки или ошибок приложений для установки ВПО, представляет собой современную форму фишинга.

Рассмотрим также и влияние киберугроз на микро- и макроуровнях экономики, на результате данных, собранных из различных источников информации [1; 6; 9]:

1. Микроуровень.
   - Финансовые потери.
     Кибератаки влияют на финансовое состояние компаний, в особенности для малого и среднего бизнеса, например, исправляя последствия влияния вредоносных ПО.
   - Угроза для бизнес-процессов.
     Атаки вирусов отнимают у пользователя продуктивное время: сбои в работе оборудования, недоступность серверов, блокировка сетей.
   - Проблемы с доверием потребителей.
     Опасения пользователей по поводу возможного мошенничества не позволяют части онлайн-пользователей совершать покупки.
   - Ухудшение репутации.
     Клиенты, инвесторы и партнёры могут потерять доверие к компании, если им станет известно о кибератаке, что в результате может привести к упадку бизнеса, а также к юридическим и финансовым последствиям.
2. Макроуровень.
   - Дестабилизация мировой экономики.
     Современная экономика охватывает множество стран и часовых поясов, поэтому сбои в одном регионе мира будут иметь волновые последствия в других регионах.
   - Нарушения в работе международных финансовых рынков.
     Сбой в системе может повлиять на финансовую стабильность или эффективность работы инфраструктуры оптовых и розничных платежей, вызвав финансовые потрясения, включая дефицит ликвидности или дефолт коммерческих банков.
   - Угроза для национальной финансовой системы.
     При тесной взаимосвязи между финансами и технологиями в цифровом обществе кибератака на какое-либо финансовое учреждение может быстро распространиться на всю финансовую систему и вызвать массовые нарушения и потерю доверия.

Приведенные выше данные, а также ряд особенностей киберрисков демонстрируют нам их трансмиссию между различными отраслями/секторами экономики, оказывая кумулятивный эффект, превосходящий размер потерь от локального влияния.

Особенно наглядной данная особенность становится на фоне современной централизации компаний и частоты обращения к аутсорсингу, который заключается в передаче части функций (включая операции или бизнес-процесс) компании внешним подрядчикам, что существенно сокращает затраты фирмы на содержание штата сотрудников различных специализаций.

Например, показательным стал рост аутсорсинга в логистике: «Пандемия COVID-19 и потребительский бум в сфере онлайн-покупок оказали положительное влияние на рынок малых грузоперевозок: многие организации, занятые в сфере электронной коммерции, стали использовать практику аутсорсинга логистических услуг с целью минимизации логистических издержек» [7, с. 366].

Также рост спроса на передачу некоторых функций компаний сторонним лицам/компаниям отмечают некоторые статистические исследования, например, исследование от NeoAnalytics гласит следующее: «В целом по итогам 2024 г. совокупный объем рынка аутсорсинга бухгалтерских услуг (включая деятельность по оказанию услуг в области бухгалтерского учета, по проведению финансового аудита и по налоговому консультированию) увеличился на 38,1% по отношению к аналогичному показателю годом ранее и составил более 500 млрд руб.» [2].

При этом несмотря на экономическую эффективность аутсорсинга, он создает риски трансмиссии киберугроз между отраслями. Например, DDoS-атака на поставщика бухгалтерских услуг нарушает работу компаний-заказчиков, демонстрируя свойство киберугроз к каскадному распространению.

Этот феномен описывается межотраслевым мультипликатором ущерба: компрометация системы управления энергоснабжением (энергетический сектор) парализует работу транспортных узлов (логистический сектор), что, в свою очередь, нарушает сроки поставок сырья для промышленных предприятий (обрабатывающий сектор) и приводит к дефициту товаров на полках магазинов (розничная торговля).

Таким образом, первоначальный инцидент запускает цепную реакцию с совокупным ущербом, многократно превышающим прямой ущерб от атаки.

Обсуждение

Ранее мы ознакомились с базовыми понятиями и сущностью киберугроз, а также раскрыли значение передовых технологий среди мошенников, которые нацелены на получение личной выгоды и предоставляют определенные услуги в области киберпреступности за деньги (CaaS) [3].

Следовательно, само собой разумеющимся в контексте темы является также рассмотрение процентного соотношения различных из киберрисков по отношению друг к другу, что вследствие поможет нам разработать перечень профилактических мер, направленных на улучшение защищенности компаний. Также считаем корректным рассмотреть темпы роста среди киберугроз в отношении компаний.

В данном случае, обращаясь к статистике ресурса Solar [5], мы можем наблюдать данное соотношение (рис. 1 и 2).

Анализ киберугроз за 2023 год выявил устойчивые тенденции: доминирование инцидентов, связанных с вредоносным ПО и эксплуатацией уязвимостей, что свидетельствует о недостаточной эффективности традиционных средств защиты.

Важно также отметить, что значительная доля срабатываний сигнатур SOC (инструменты, отслеживающие угрозы, атаки и мгновенно реагирующие на инциденты) подтверждает работоспособность мониторинга, но одновременно подчеркивает их неспособность противостоять целевым атакам, требующим поведенческого анализа.

Значительное внимание в том числе вызывает высокий уровень компрометации учетных записей и несанкционированного доступа, демонстрирующий системные пробелы в управлении идентификацией.

Данные за 2024 год подтверждают преемственность тенденций: сохраняется доминирование атак через вредоносное ПО и эксплуатацию уязвимостей, что свидетельствует о системных проблемах в управлении безопасностью.

Высокие показатели срабатывания сигнатур SOC демонстрируют как работоспособность систем мониторинга, так и их неэффективность против целевых атак и угроз нулевого дня. Критической остается ситуация с несанкционированным доступом и компрометацией учетных записей, что указывает на остающиеся фундаментальные пробелы в управлении доступом.

Несмотря на стабилизацию векторов атак, наблюдается количественный рост инцидентов с 6 до 9,5 тысяч за 2024 год (рис. 3), что свидетельствует об эскалации киберугроз. Сохраняющиеся угрозы — сетевые и веб-атаки, использование нелегитимного ПО — подтверждают успешную эксплуатацию злоумышленниками базовых пробелов в безопасности.

Исходя из вышеописанного мы можем предположить несколько вариантов, которые потенциально могут объяснить рост числа инцидентов, сопряженных с увеличением издержек вследствие киберрисков (финансовые потери, возникшие из-за кибератак, утечек данных и т. д.):

1. усложнение инструментария киберпреступности за счет прогресса в области технологий;
2. коммерциализация киберпреступности;

Рис. 1. Распределение всех инцидентов по типам киберугроз в 2023 году.

Рис. 2. Распределение всех инцидентов по типам киберугроз в 2024 году.

3. накопительный эффект множества уязвимостей в системе;
4. усовершенствование систем обнаружения киберугроз.

Выводы

Таким образом, мы можем сформулировать ключевые выводы и рекомендации, которые в будущем способны сократить число киберугроз и оказываемое ими критическое воздействие на информационный и экономический суверенитет как на микро-, так и на макроуровнях.

В первую очередь наша гипотеза нашла свое подтверждение и в условиях современности киберугрозы действительно эволюционировали в качественно новую угрозу — они характеризуются не точечным, а комплексным и каскадным влиянием, способным не только подорвать финансовое состояние конкретных корпораций, но и деформировать конкурентную среду, а в перспективе - поставить под вопрос экономическую независимость и безопасность страны.

В динамике 2023–2024 годов наблюдается установление общих тенденций в области киберрисков, которые также позволяют нам сформулировать общий перечень практических рекомендаций, целью которых является кратное уменьшение вероятности возникновения киберугроз.

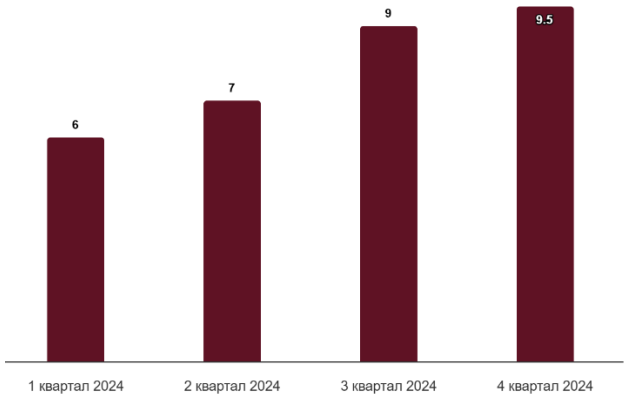

Рис. 3. Распределение инцидентов по кварталам в 2024 году, тыс. шт.

Во-первых, необходимо внедрить систему гослицензирования критического ПО, предусматривающую распространение отечественного программного обеспечения через уполномоченные органы с возможностью оперативного блокирования лицензий.

Во-вторых, ввести обязательный аудит информационной безопасности для системообразующих предприятий с привлечением аккредитованных компаний-аудиторов для организаций с ограниченными ресурсами.

В-третьих, необходимо создать отраслевые центры мониторинга и противодействия кибератакам для координации действий и оперативного обмена информацией об угрозах.

Реализация указанных рекомендаций, при всей своей ресурсоемкости, является экономически оправданной, так как направлена на защиту системообразующих компаний — основы экономического суверенитета страны.

В долгосрочной перспективе инвестиции в создание целостной системы кибербезопасности позволяют избежать катастрофических издержек, связанных с восстановлением после атак на критическую инфраструктуру, и обеспечивают устойчивость национального хозяйства в условиях цифровизации.

Библиографический список

1. *Алексеев Е. В.* Моделирование влияния кибератак на экономическую стабильность // Инновации и инвестиции. — 2024. — № 4. — С. 375—377.
2. Анализ российского рынка аутсорсинга бухгалтерских услуг: итоги 2024 г., прогноз до 2028 г. / NeoAnalytics, Магазин исследований. — URL: https://marketing.rbc.ru/articles/15879/ (дата обр. 15.04.2026).
3. *Андриянова А.* Преступность как услуга: как хакерство превратилось в глобальный бизнес по подписке / Компьютерра. — URL: https://www.computerra.ru/317586/prestupnost-kak-usluga-kak-hakerstvo-prevratilos-v-globalnyj-biznes-po-podpiske/ (дата обр. 15.11.2025).
4. *Антропов К. Ю.* Кибербезопасность и сохранение цифрового суверенитета экономики // Вестник экономической безопасности. — 2021. — № 5. — С. 268—273.
5. *Вятника А.*, *Осипова А.* Актуальные киберугрозы: I–II кварталы 2025 года // Positive Technologes. —. — URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/#id1 (дата обр. 25.01.2026).
6. Кибератаки на российские компании в 2024 году / Solar. — URL: https://rt-solar.ru/analytics/reports/5320/ (дата обр. 15.04.2026).
7. *Кудина А. В.*, *Лахтина Е. П.*, *Савин Г. В.* Аутсорсинг в логистике // Россия: тенденции и перспективы развития. — 2021. — № 16—1. — С. 366—368.
8. *Рожков Р.* Шантаж и шпионаж: какие киберриски угрожают бизнесу и пользователям в 2025 году / Forbes. — URL: https://www.forbes.ru/tekhnologii/531090-santaz-i-spionaz-

kakie - kiberriski - ugrozaut - biznesu - i - pol - zovatelam - v - 2025 - godu (дата обр. 15.04.2026).
9. *Струнин Д. А.* Кибератаки и их влияние на цифровую экономику // Молодой ученый. — 2023. — 5 (452). — С. 15—16.
10. *Халин В. Г.*, *Чернова Г. В.* Цифровизация и киберриски // Управленческое консультирование. — 2023. — 7 (175). — С. 28—41.